

ABSTRACT

A system and method for preventing illegal use of software is provided, which cannot be analyzed by using a software debugger which operates in any mode, and the
5 secret information stored in which cannot be retrieved even if backup data of the secret information is stored in another device. The system comprises a unit for storing secret information; a unit for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means; a unit for determining whether an illegal access to the system is performed; and a cryptosystem key updating
10 unit for providing the same key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if the illegal access determining means detects no illegal access, or providing different keys for the above two kinds of cryptosystem keys if the illegal access determining
15 means detects an illegal access, and wherein the cryptosystem key updating units updates the above two kinds of cryptosystem keys for each access to the system.

09303561 060399